UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE CAPITAL ONE CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 1:19-md-2915 (AJT/JFA)
This Document Relates ONLY to the following Case: MARCUS MINSKY, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. CAPITAL ONE FINANCIAL CORPORATION, RICHARD FAIRBANK, ROBERT ALEXANDER, and MICHAEL JOHNSON, Defendants.	Case No. 1:19-cv-1472 (AJT)

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS'
MOTION TO DISMISS THE AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

On July 29, 2019, Capital One Financial Corporation ("Capital One" or the "Company") announced that it had been targeted in a criminal cyber-attack in which a hacker stole personal information of approximately 106 million Capital One credit card customers and applicants (the "Cyber Incident"). The suspected perpetrator is in custody and, to date, there is no indication that the information has been disseminated or used to commit fraud or identity theft. The day after Capital One announced the Cyber Incident, the Company's stock price fell by less than 5%, but has since more than fully recovered, and is up ***nearly 13%*** since the July 30, 2019 close.

Plaintiff's Complaint seeks to manufacture claims that the Company and three executives violated federal law by making statements that are alleged to have misled investors. But as shown below, the Complaint falls far short of satisfying the exacting pleading standards imposed by the Private Securities Litigation Reform Act of 1995 (the "PSLRA") and therefore must be dismissed. The crux of Plaintiff's claims is that certain statements touching on matters of data security or Capital One's "digital transformation" were misleading because the Company "sacrificed cybersecurity" to optimize execution on its "information-based strategy." But hindsight-driven, conclusory allegations that Capital One should have had "better" data security do not plead a claim that the challenged statements were false or misleading at all, let alone at the time they were made.

Further, many of the statements challenged in the Complaint are not investor-facing and do not even address data security. Plaintiff attacks general compliance policies that fail even to mention cybersecurity, while those that do—including those describing cybersecurity as "incredibly important," "critical," or a "top priority"—are immaterial "puffery" upon which no reasonable investor would base a decision to purchase stock. Plaintiff also attacks cardholder

privacy notices that were not directed to Capital One investors and are therefore not actionable because they were not made "in connection with" a purchase of securities.

Separately dooming his claims, Plaintiff also fails to plead particular facts that raise the required strong inference that Defendants acted with scienter, *i.e.*, intent to deceive or *severe* recklessness. Instead, Plaintiff relies on conclusory, boilerplate allegations that courts have rejected time and again. These allegations fail to specifically tie the Individual Defendants (or any Capital One representative accused of making a false statement) to awareness of information conflicting with the challenged statements or even suggesting that those statements might mislead reasonable investors. Plaintiff's failure to plead facts connecting the speakers to knowledge of such contradictory information dooms Plaintiff's "fraud" claims and requires dismissal independently of the Complaint's other pleading deficiencies.

For all of these reasons, Plaintiff's Complaint fails to state a claim for violation of Section 10(b) of the Securities Exchange Act of 1934, and Plaintiff's failure to plead a Section 10(b) claim means that Plaintiff likewise has not stated a claim under Section 20(a). As such, the Complaint must be dismissed in its entirety.

II. SUMMARY OF PLAINTIFF'S ALLEGATIONS

A. The Parties

Capital One is a Virginia-based financial services company whose common stock trades on the New York Stock Exchange. Amended Complaint ("AC") ¶¶ 23, 26. Defendant Richard Fairbank is Capital One's Founder and Chief Executive Officer. *Id.* ¶ 27. Defendant Robert Alexander is Capital One's Chief Information Officer ("CIO"). *Id.* ¶ 28. Defendant Michael Johnson served as Capital One's Chief Information Security Officer ("CISO") from March 2017 until November 2019. *Id.* ¶ 29. The plaintiff who commenced this action, Marcus Minsky, held

fewer than five shares of Capital One common stock.[1] Mr. Minsky's lawyers subsequently replaced him with Plaintiff Edward Shamoon—the only lead plaintiff applicant in this case—who claims to have purchased 250 shares of Capital One common stock on September 6, 2018 for $98.25/share, which he continues to hold. *See* Dkts. 216-3 & 216-4. Mr. Shamoon seeks recompense for a temporary "paper loss" on his investment, but as of the market close on the date of this filing, Capital One's shares were trading ***5% above*** the price at which Mr. Shamoon bought.

B. Capital One's Well-Publicized "Information-Based" Business Strategy

As alleged throughout the Complaint, Capital One has for decades publicly and candidly discussed its pursuit of an "information-based strategy" leveraging extensive analysis of consumer data to identify desirable customers, effectively market products and services, make more informed credit decisions, offer superior customer service, and grow its profitability. *See, e.g.*, AC ¶¶ 7, 37–42, 114. As Plaintiff alleges, as far back as 1996, in Capital One's first publicly filed annual report on SEC Form 10-K, the Company stated:

> The Company's IBS [*i.e.*, Information Based Strategy] is designed to allow the Company to differentiate among customers based on credit risk, usage and other characteristics and to match customer characteristics with appropriate product offerings. . . . By using sophisticated statistical modeling techniques, the Company is able to segment its potential customer lists based upon the integrated use of credit scores, demographics, customer behavioral characteristics and other criteria.. . . . ***The Company applies IBS to all areas of its business*** . . . .

Id. ¶ 37 (emphasis added).

Plaintiff alleges that Capital One's information-based strategy depended on amassing large stores of data, including consumer data, to be analyzed in driving decisions about marketing, product and service development, extension of credit, and customer service. *See, e.g., id.* ¶ 115 ("Machine learning requires data . . . . [T]he more data Capital One makes available to its machine

[1] *See* Case 1:19-cv-01472-AJT-JFA, Document 1-1.

learning programs, the more accurate – and therefore useful – those programs will be."). Plaintiff acknowledges that Capital One repeatedly discussed this aspect of its strategy in public statements. *See id.* ¶¶ 41–42, 72, 77, 79, 92.

C. The Criminal Cyber-Theft Of Certain Capital One Data In The Cyber Incident

Plaintiff alleges that, in March and April 2019, hacker Paige Thompson obtained unauthorized access to a Capital One server containing a significant store of consumer data. *Id.* ¶¶ 171-74. Plaintiff alleges that Capital One had a "Web Application Firewall ("WAF")" in place, which was intended to shield its servers from such "malicious attacks." *Id.* ¶ 151. Plaintiff further alleges that "[a] WAF uses programmed rules to distinguish between legitimate access requests, which it permits, and illegitimate access requests, which it denies" (*id.*¶ 152) and that "[i]f a request is legitimate, then the WAF automatically assigns the requester a role" and related access credentials. *Id.* ¶ 153. Plaintiff acknowledges that "[i]f properly implemented, a WAF should deny access to all entrants except those who have already been approved. But Capital One's WAF was misconfigured, allowing access to malicious outsiders under certain circumstances." *Id.* ¶ 154. Plaintiff also acknowledges that the consumer data on Capital One's server was encrypted and that Capital One had taken the further security measure of "tokeniz[ing]" the vast bulk of the most sensitive data (social security numbers and bank account numbers). *Id.* ¶ 175-76. Plaintiff alleges that upon gaining access to Capital One's servers, "Thompson was assigned credentials that automatically decrypted all the data available." *Id.* ¶ 175.

Plaintiff alleges that, "[o]n April 21[, 2019], Thompson exfiltrated the data to outside of Capital One's firewall." *Id.* ¶ 179. But Plaintiff alleges that Thompson "had no plans to monetize" the data she stole and implicitly acknowledges that, to date, neither Capital One nor law enforcement have uncovered any evidence that the data was used for fraud, sold, or otherwise

disseminated. *Id.* ¶¶ 186-88. Capital One issued a press release publicly reporting the Cyber Incident on July 29, 2019, shortly after learning that it had occurred. *Id.* ¶¶ 11, 189.

D. Plaintiff's Claims and Allegations

The Complaint asserts claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, 15 U.S.C. §§ 78j(b), 78t(a), and SEC Rule 10b-5, 17 C.F.R. § 240.10b-5. Plaintiff alleges these claims on behalf of a putative class of investors who purchased or otherwise acquired Capital One common stock between July 23, 2015 and July 29, 2019. AC ¶ 1. The Complaint groups the statements into six categories (*see* headings A. through F. of Section VIII, "Defendants' False and Misleading Statements," beginning at AC p. 46). Defendants will use the Complaint's groupings except as noted below. For the Court's convenience, Defendants attach as Exhibit 1 hereto a chart listing each of the 28 statements Plaintiff challenges.

Plaintiff's first category (the "Legal Obligations/Industry Practices" statements) challenges statements that Plaintiff characterizes as addressing Capital One's compliance with legal, regulatory, and industry-based standards for protecting customer data (AC ¶¶ 208, 210; Ex. 1, Stmts. 1-2). In addressing this category of statements, Defendants will also address the last two statement categories which also relate to compliance with industry practices (AC Sections VIII.E. & VIII.F., relating to encryption and data access/retention respectively) (AC ¶¶ 249-53, 255-56; Ex. 1, Stmts. 22–28). The second category Plaintiff challenges (the "Risk Factor Statements") consists of risk factor statements in Capital One's 2015-2018 Forms 10-K (AC ¶ 218; Ex. 1, Stmt. 3). Although Plaintiff does not specify any particular language in the Risk Factor Statements alleged to have misled investors, his theory appears to be that the statements "warned identically of cybersecurity risks" and thus were not sufficiently "tailored to Capital One." *Id.* The third category (the "Digital Transformation Statements") consists of statements that the Company's "digital transformation" would have a positive impact on, among other areas of its business,

"regulatory compliance," "risk management," and "cybersecurity." AC ¶¶ 223, 225-29; Ex. 1, Stmts. 4–9. Plaintiff's fourth category of statements (the "Priority Statements") describe Capital One's cybersecurity efforts as a "top priority"—or as "critical" or "incredibly important." AC ¶¶ 210, 232-38, 241-45; Ex. 1, Stmts. 10–21.

Plaintiff generally alleges that the above categories of statements were false and misleading because Capital One "sacrifice[ed] cybersecurity" to optimize execution on the Company's information-based strategy by creating "large data pools" and "granting widespread [internal] access" to the data. *Id.* ¶¶ 211, 222, 230, 239, 246, 254; *see also id.* ¶¶ 2, 118, 258. Plaintiff also alleges that the challenged statements were false or misleading because Capital One failed to adequately encrypt data and monitor system requests for access to data and that, as a result of the foregoing, the Company "violat[ed] a host of industry practices and ethical standards." *Id.* ¶¶ 211, 222, 230, 239, 246, 254, 258.

III. LEGAL STANDARDS

To state a claim under Section 10(b) and SEC Rule 10b-5, Plaintiff must allege and ultimately prove six elements: (1) a material misrepresentation or omission of material fact; (2) scienter; (3) a connection with the purchase or sale of a security; (4) reliance; (5) economic loss; and (6) loss causation. *See Dura Pharms., Inc. v. Broudo*, 544 U.S. 336, 341-42 (2005). Plaintiff's claims are subject to the heightened pleading standards of Rule 9(b) and the PSLRA. Rule 9(b) provides that in "alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b). In enacting the PSLRA, Congress determined it was necessary to raise the bar even higher than Rule 9(b) for securities class actions. *See Maguire Fin., LP v. PowerSecure Int'l, Inc*., 876 F.3d 541, 546 (4th Cir. 2017). The PSLRA requires that Plaintiff "specify each statement alleged to have been misleading, the reason or

reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, … state with particularity all facts on which that belief is formed." 15 U.S.C. § 78u-4(b)(1). The PSLRA also requires Plaintiff to "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." *Id*. § 78u-4(b)(2)(A). The "required state of mind" is scienter, defined to mean "a mental state embracing intent to deceive, manipulate, or defraud." *Tellabs, Inc. v. Makor Issues & Rights, Ltd*., 551 U.S. 308, 319 (2007) (internal quotation marks and citation omitted). A "strong inference" of scienter is one that is "more than merely plausible or reasonable—it must be cogent and at least as compelling as any opposing inference of nonfraudulent intent." *Id*. at 314.

IV. ARGUMENT

A. Plaintiff Fails To Plead That The Challenged Statements Were False, Misleading, Or Otherwise Actionable Under Section 10(b).

Plaintiff asserts extremely serious claims of federal securities fraud against Capital One and the Individual Defendants—claims subject to rigorous, heightened pleading standards. Yet in support of these weighty claims, Plaintiff merely attacks statements that (1) do not relate directly (or sometimes at all) to cybersecurity, (2) accurately disclose the very security risks at issue; (3) constitute non-actionable puffery or opinion/belief statements not adequately pled to have been false; and/or (4) were made in customer-facing privacy policies or by non-Defendants at various conferences. As discussed in detail in the sections that follow, these statements—either analyzed individually or in the aggregate—are not adequately pled to have been misleading to reasonable investors, much less false, and therefore, fall woefully short of Plaintiff's high pleading hurdle.

1. The Legal Obligations/Industry Practices Statements

The Legal Obligations/Industry Practices Statements concern (i) "compliance risk management" (Ex. 1, Stmt. 1); and (ii) statements to consumers (not investors) that the Company

will protect their information "with controls based upon internationally recognized security standards, regulations, and industry-based best practices" (*id.* Stmt. 2). Plaintiff also challenges statements about data encryption (*id.*, Stmts. 22-26) and data access/retention (*id.*, Stmts. 27-28).

a) Plaintiff Fails To Plead Facts Establishing The Statements Were False Or Misleading.

Plaintiff asserts the same conclusory explanation as to why all of these statements were purportedly false or misleading—that Capital One "creat[ed] dangerously large data pools, grant[ed] widespread access…, fail[ed] to monitor data requests," did not effectively "encrypt data on its server," and its "retention period and data scope did not comply with the customer's [sic] reasonable expectations." AC ¶¶ 211, 254, 258. Plaintiff repeats this refrain throughout the Complaint but fails to plead facts supporting a claim that the statements Plaintiff challenges misled investors for the reasons asserted (or at all).

In fact, Plaintiff's own allegations confirm that Capital One repeatedly emphasized in public statements that the Company was collecting consumer data to further its information-based strategy and was analyzing and using that data "across all the segments" of its business. *Id.* ¶ 41; *see also id.* ¶ 72 ("Capital One executives consistently referred to … [Capital One's] use of machine learning employed on vast sets of customer data …."); ¶ 77 (discussing "this data foundation … we've been putting into place"); ¶ 92 (discussing the "big opportunity… to ultimately increasingly leverage the big data that is out there"). These allegations directly negate Plaintiff's conclusory and unsupported assertion that Defendants misled investors about Capital One's creation of "data pools" and "widespread access" to the data within the Company.

Plaintiff similarly fails to plead any factual support for the assertion that Capital One's data retention practices failed to "comply with … customer[s'] reasonable expectations." Not only does Plaintiff fail to plead *any* factual basis establishing what customers "expect[ed]," Plaintiff's

conclusory allegation on this point is flatly at odds with the numerous public statements Plaintiff acknowledges Capital One made about its use of consumer data to further its information-based strategy. Further, even if Plaintiff had pled facts supporting an alleged failure to adhere to *customer* expectations (he has not), that cannot be equated to knowingly defrauding *investors*, which is what Plaintiff must plead here. *See In re Citigroup, Inc. Sec. Litig*., 330 F. Supp. 2d 367, 380 & n.5 (S.D.N.Y. 2004) (differentiating between an "intent to defraud [Defendant's] shareholders" and intent to "hide matters from the shareholders of [Defendant's] clients").

Plaintiff's allegations that Capital One "fail[ed] to monitor data requests" fare no better. Here again, Plaintiff is undone by his own allegations pleading that "Capital One suffered upwards of 20 cyberattacks per month," which were reported up the chain of command to Defendant Johnson at regularly held meetings. AC ¶¶ 149, 150. Such attacks would not have been detected if Capital One was not monitoring data requests. Plaintiff is thus left with the hindsight and conclusory allegation that "a competent network should have been able to detect when the hacker exfiltrated large amounts of data from Capital One's server." *Id.* ¶ 147. This too fails to plead falsity, because a court cannot infer that Capital One's monitoring practices were inadequate from the fact that that Company was victimized in a cyber-attack. *See In re Heartland Payment Systems, Inc. Sec. Litig.*, Civ. No. 09-1043, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009); *see also Oklahoma Firefighters Pension & Ret. Sys. v. K12, Inc.*, 66 F. Supp. 3d 711, 717 (E.D. Va. 2014) (Trenga, J.) (statements admitting that "in hindsight, [the company] realized that its marketing activities were not done in the most effective manner" did not render prior statements regarding company's focus on marketing false when made).

Plaintiff's allegations that the data encryption Capital One employed effectively amounted to "no encryption at all" also fail to support fraud claims. Plaintiff's allegations acknowledge that

Capital One *did* encrypt data and took the further step of tokenizing social security and bank account numbers. AC ¶¶ 175-76. Plaintiff merely alleges that Capital One's data encryption was "not meaningful[]" because a hacker was able to exploit a "misconfigured WAF [Web Application Firewall]" to fraudulently obtain decrypting credentials. *Id.* ¶¶ 154, 175. But this allegation, and Plaintiff's related assertion that "Capital One's . . . access policies . . . and automatic decryption made a hack like the Data Breach inevitable" (*id.* ¶ 17), impermissibly seek to plead "fraud by hindsight." *Hillson Partners,* 42 F.3d 204, 209 (4th Cir. 1994) ("Mere allegations of 'fraud by hindsight' will not satisfy the requirements of Rule 9(b)."). Another federal court rejected similar allegations and dismissed securities fraud claims in *Heartland*. *See* 2009 WL 4798148, at *5. There, the plaintiffs alleged that the defendant payment processing company misrepresented the state of its data security prior to a cyber-attack that resulted in the theft of 130 million credit and debit card numbers, contending that the breach proved that those statements had been false or misleading. *Id.* at *4-6. The court dismissed the claims, holding that "[t]he fact that a company has suffered a security breach does not demonstrate that the company did not 'place significant emphasis on maintaining a high level of security.'" *Id.* at *5. The same rationale applies here—where Plaintiff expressly *concedes* that Capital One encrypted (and tokenized) data, but alleges that the encryption was overcome due to a misconfigured WAF.

Even if Plaintiff had pled sufficient factual support for his criticisms of Capital One's data security practices (and he has not), the Complaint still fails to adequately plead that such criticisms caused the statements Plaintiff challenges to mislead Capital One's investors. *See In re Target Corp. Sec. Litig.,* 275 F. Supp. 3d 1063, 1071 (D. Minn. 2017) (dismissing complaint where plaintiff failed to "connect … specific [alleged] problems to … specific statements"). For instance, the challenged "Compliance Risk Management" disclosures in Capital One's 2015-2018 Forms

10-K refer to the Company's efforts to "adjust" its compliance risk program to "fully address" the changing expectations of regulators and customers. AC ¶ 208; Ex. 1, Stmt. 1. To the extent that this statement can even be read as addressing cybersecurity (as opposed to the vast body of legal and regulatory requirements with which all financial institutions must comply), Plaintiff has not pled a single particular fact showing that Capital One did *not* "evaluate the regulatory environment" and "adjust" its "compliance risk program" in order to "address these expectations." None of Plaintiff's criticisms of Capital One's data practices—*i.e.*, that the Company created "large data pools, grant[ed] widespread access, and fail[ed] to monitor data requests," *see id.* ¶ 211—contradict or even relate to Capital One's general statements about its compliance risk management program. *See In re First Union Corp. Sec. Litig.*, 128 F. Supp. 2d 871, 887, 893 (W.D.N.C. 2001) (plaintiff failed to plead falsity merely by referring to a "laundry list" of alleged "problems").

Plaintiff's allegations challenging (1) an excerpt of Capital One's "Online & Mobile Privacy Statement," which informs consumers visiting Capital One's website that Capital One "will protect [your] information with controls based upon internationally recognized security standards, regulations, and industry-based best practices" (AC ¶ 210; Ex. 1, Stmt. 2); and (2) the statement in Capital One's annual privacy notice that "we use security measures that comply with federal law . . . includ[ing] computer safeguards and secured files and buildings" (AC ¶ 253, Ex. 1, Stmt. 26) are similarly deficient. To adequately plead the falsity of the Online Mobile & Privacy Statement, Plaintiff would have to allege particular facts establishing that Capital One did not have security controls, or that the controls were not "based upon" international and industry standards—

which he has not done. As for the annual privacy notice, Plaintiff has not alleged that Capital One did *not* use "computer safeguards and secured files and buildings."[2]

To the extent Plaintiff claims that Capital One's cybersecurity practices violated a "regulatory requirement" or "internationally recognized" standard—or that its security measures did not "comply with federal law," Plaintiff must specify which requirement, standard, or law was violated and plead facts establishing the alleged violation. *See, e.g., In re PEC Sols. Sec. Litig.*, 2004 WL 1854202, at *12 (E.D. Va. May 25, 2004) (rejecting conclusory allegations based on GAAP violations because plaintiffs "fail to allege why [the] reports are violations of GAAP and how the reports violated the rules"), *aff'd* 418 F.3d 379 (4th Cir. 2005). Although Plaintiff refers to certain standards and industry practices, he does not plead facts establishing any failure by Capital One to comply with them, or that its security controls were not "based on" such standards.

The only two standards Plaintiff asserts were violated are the CFPB's principles on data security (the "CFPB Principles" *see* Ex. 1, Stmts. 27-28) and the Payment Card Industry ("PCI") Security Standards Council's Requirements. *See* AC ¶¶ 204-06, 255-58. Plaintiff alleges that Capital One violated the PCI Requirements' data retention guidelines by having "unreasonably long retention periods," but as Plaintiff alleges, the PCI Requirements say that retention time should be commensurate with "business requirements." *Id.* ¶ 206. The same is true of the PCI Requirements' access provisions, which state that access should be provided "to only those individuals whose job requires" it. *Id.* ¶ 207. But Plaintiff's own allegations affirmatively plead that Capital One amassed and retained data and made it accessible across all of the Company's segments for the business purpose of optimizing execution on the information-based strategy the

[2] Because Stmts. 2 and 26 were directed to *consumers* rather than *investors*, they are not actionable under the securities laws in any event because the statements were not made "in connection with" a security purchase. *See* section IV.A.5, *infra*.

Company's public statements to investors repeatedly emphasized. *See* ¶¶ 114-17 (alleging that "Capital One had to create data lakes and make their data accessible" to optimize the "machine learning" the Company used to develop and target marketing strategies, make credit decisions, and support card fraud detection and prevention efforts benefitting Capital One's customers). The CFPB Principles say that retention periods should be "consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected" (*id.* ¶ 257), and, as noted, Plaintiff has not adequately pled that Capital One's retention practices were inconsistent with such reasonable consumer expectations. *See supra*, at 8-9.

b) Most Of The Legal Obligations/Industry Practices Statements Are Immaterial Puffery.

The Fourth Circuit has consistently held that rosy, non-specific statements of opinion regarding corporate performance cannot form the basis of Section 10(b) liability. *See Longman v. Food Lion, Inc.*, 197 F.3d 675, 685 (4th Cir. 1999). These "rosy affirmation[s] commonly heard from corporate managers and familiar to the marketplace . . . are so vague, so lacking in specificity, or so clearly constituting the opinions of the speaker, that no reasonable investor could find them important to the total mix of information available." *In re Cable & Wireless, PLC*, 321 F. Supp. 749, 766 (E.D. Va. 2004). Here, Plaintiff challenges several general and non-specific statements describing Capital One's commitment to complying with regulatory and consumer expectations, *see, e.g.*, Ex. 1, Stmt. 1 ("[W]e continuously evaluate the regulatory environment and proactively adjust our compliance risk program to fully address these expectations"); touting the quality of Capital One's cyber security practices, *id.*, Stmt. 25 ("[W]e believe we have a robust suite of

authentication and layered information security controls."); and discussing "alignment" with CFPB Principles, *id.*, Stmts. 27-28.[3]

Numerous courts have concluded that analogous statements are immaterial as a matter of law. *See, e.g.*, *K12*, 66 F. Supp. 3d at 718-19 (statements that company "did an 'amazing job' ensuring compliance," that it "took 'compliance very seriously,'" and "used a 'sophisticated approach' to ensure compliance 'with every rule and regulation'" are puffery because they cannot be objectively demonstrated as false or misleading). The Second Circuit also recently held strikingly similar compliance statements to be immaterial as a matter of law. *See Singh v. Cigna Corp.*, 918 F.3d 57, 62-63 (2d Cir. 2019). In *Singh*, the Second Circuit found that references to a company's "unwavering commitment" to compliance and claims that it "ha[d] established policies and procedures to comply with applicable requirements" were immaterial puffery, characterizing the plaintiff's complaint as a "creative attempt to recast corporate mismanagement as securities fraud" by utilizing "banal and vague corporate statements" and then "point[ing] to significant regulatory violations." 918 F.3d at 59-61, 63-64. Here, in contrast to *Singh, Plaintiff does not allege any regulatory violations or findings of noncompliance by Capital One*, making Plaintiff's allegations *far less compelling* than those that the Second Circuit held were inadequate in *Singh*.

The Second Circuit in *Singh* also found it significant that (i) the company's compliance statements were "framed by acknowledgments of the complexity and numerosity of applicable regulations," which "suggests caution (rather than confidence) regarding the extent of [the

[3] Plaintiff's claims predicated on Stmts. 1, 2, 25–26, & 27–28 must be dismissed for the independent reason that these statements include non-verifiable opinion/belief statements. To allege the falsity of such statements, the Complaint must "allege that the opinion[s] expressed w[ere] different from the opinion[s] actually held by the speaker." *Teamsters Local 210 Affiliated Tr. Fund v. Neustar, Inc.*, No. 1:17-cv-1145-AJT-JFA, 2019 WL 693276, at *4 (E.D. Va. Feb. 19, 2019) (internal citation and quotation marks omitted) (Trenga, J.). Plaintiff fails to do so here.

company's] compliance." *Id.* at 64. The Court also noted that the company disclosed it would "allocate significant resources" to compliance, which "suggests a company actively working to improve its compliance efforts, rather than one expressing confidence in their complete (or even substantial) effectiveness." *Id.* Similarly here, Capital One explicitly warned investors that it is "subject to a variety of continuously evolving and developing laws and regulations in the United States and abroad regarding privacy, data protection and data security"; that "[s]ignificant uncertainty exists as privacy and data protection laws may be interpreted and applied differently from country to country"; and noted that its compliance efforts "entail substantial expenses." *See, e.g.*, Ex. A[4] at 25 (referenced at AC ¶ 218).

The Eleventh Circuit's recent ruling in *Carvelli v. Ocwen Financial Corporation* also supports a finding that the regulatory compliance/alignment statements Plaintiff challenges are immaterial and legally not actionable. *See* 934 F.3d 1307, 1321-22 (11th Cir. 2019). In *Ocwen*, the Eleventh Circuit rejected similar challenges to statements that a company devoted "substantial resources to regulatory compliance and risk management efforts" and felt "good about the progress" towards "national mortgage settlement compliance" despite the fact that various regulators subsequently filed actions charging lack of compliance. 934 F.3d at 1321-22. Here, statements generally avowing compliance with regulatory standards, industry practices, and consumer expectations are similarly non-actionable.

Capital One's statement that it had a "robust suite" of security tools including encryption and tokenization (Ex. 1, Stmt. 25) is also non-actionable puffery. Indeed, a court in another securities case arising out of purported cybersecurity issues recently concluded that statements discussing a company's "robust multifactor verification" and "hardware-based security," and

[4] Cites to "Ex. _" refer to exhibits to the Declaration of Benjamin Lee filed herewith.

stating that its computer chips were "optimized particularly for data protection" constituted immaterial puffery because they were only "vague positive statements." *In re Intel Corp. Sec. Litig.*, No. 18-cv-00507-YGR, 2019 WL 1427660, at *9 (N.D. Cal. Mar. 29, 2019).

2. The Risk Factor Statements

Bizarrely, Plaintiff also challenges statements *warning investors* of the *very risk* that occurred here—a cybersecurity intrusion. *See* AC ¶ 218; Ex. 1, Stmt. 3. The Risk Factor Statements, found in Capital One's Forms 10-K, provide *pages* of specific warnings relating to cybersecurity. *See* Exs. A-D. Plaintiff fails to specify any portion of the Risk Factor Statements that he alleges are misleading, which, alone, supports dismissal of Plaintiff's claims challenging these statements, because the PSLRA requires far greater specificity. *See In re 2007 Novastar Fin. Inc., Sec. Litig.*, 579 F.3d 878, 882-83 (8th Cir. 2009) (dismissing claims where complaint lacked "any indication as to what specific statements within these communications are alleged to be false or misleading"). Plaintiff appears to assert that the warnings were misleading for failing to disclose: (1) that Capital One was "sacrificing cybersecurity" by pursuing its Information-Based Strategy; and (2) that Capital One faced a "particular risk" from "overbroad access granted to presumed insiders." AC ¶ 222. These allegations fail to adequately plead falsity.

First, the Risk Factors disclosed the very dangers to which Plaintiff attributes his losses. They warned, for example, that Capital One "continue[s] to be the subject of attempted unauthorized access" and that "any one or combination" of its security protections "could fail to detect, mitigate or remediate these risks in a timely manner." *See, e.g.*, Ex. A at 24. Far from guaranteeing that its systems were impenetrable, Capital One warned investors that its protections could prove insufficient to thwart a determined criminal hacker. These statements "remind[ed] [investors] of inherent risks," and "it would seem strange" that warnings to investors "would be actionable under securities law." *Phillips v. Triad Guar. Inc.*, No. 1:09-CV-71, 2015 WL 1457980,

at *11 (M.D.N.C. Mar. 30, 2015). *See also Veal v. LendingClub Corp.*, No. 18-cv-02599-BLF, 2019 WL 5698072, at *15 (N.D. Cal. Nov. 4, 2019) (risk factors that accurately disclosed the company's state of affairs were not actionable).[5]

Second, Plaintiff fails to adequately plead that the Risk Factor Statements were misleading by omitting a "particular risk" of allegedly "overbroad" internal access to data within Capital One. Plaintiff premises this assertion on four "incidents" that Capital One reported under Montana law.[6] *See* AC ¶ 220. Critically, Plaintiff does not allege that these events bear any resemblance whatsoever to the Cyber Incident at issue in this case. Far from it—rather than relating to an external hack of computer systems, the *public* Montana filings that Plaintiff cites discuss one-off instances of Capital One employees misusing customer account information accessed in the course of their employment. *See* Ex. E at 1, 5, 9, 13, excerpts of public notices, *available at* https://dojmt.gov. Plaintiff also does not plead any particular facts suggesting that the misbehaving employees were given access to customer data *without a reasonable business purpose*; instead, the documents reflect that they misused information accessed in the course of performing their jobs. Further, Capital One's risk disclosures expressly warned of precisely the risk that occurred in these Montana incidents by discussing security risks resulting from "malice on the part of our employees." Ex. A at 24. Finally, Plaintiff alleges that notice of the occurrence of the Montana incidents was posted publicly on the Montana Department of Justice's website. AC ¶ 220. Thus,

[5] Moreover, the potential risk disclosed—a significant cybersecurity breach—had not yet occurred when the challenged statements were made, further undermining Plaintiff's allegations of falsity. *See Doyun Kim v. Advanced Micro Devices, Inc*., No. 5:18-cv-00321-EJD, 2019 WL 2232545, at *7 (N.D. Cal. May 23, 2019) (allegations challenging cybersecurity risk disclosures failed to plead a claim where "the potential risks disclosed in the SEC filings had not come to fruition when Defendants filed the challenged risk disclosures").

[6] Montana law requires disclosure of "any breach" involving the personal information of "any resident of Montana." Mont. Code Ann. § 30-14-1704. Unlike the securities laws, this statute contains no materiality threshold.

to the extent these incidents illuminate risks posed by Capital One's practices, they were publicly reported, not "concealed."[7] Moreover, nothing about these Montana incidents involving one-off insider misdeeds demonstrates that Capital One's perimeter defenses and cybersecurity protections against external threats were so inadequate that Defendants' public statements about them defrauded investors.

3. The Digital Transformation Statements

The Digital Transformation Statements are a random grab bag of statements that Plaintiff alleges gave the misleading impression that the "digital transformation . . . was a 'shared path' which led to better cybersecurity," or that the "benefits [of] the digital transformation went hand in hand" with cybersecurity. AC ¶¶ 223, 230. Plaintiff again repeats the refrain that "Capital One compromised cybersecurity" in service of "machine learning." *Id.* ¶ 230. But the Digital Transformation Statements are vague and untethered to any particular cybersecurity practice or deficiency cited in the Complaint. For instance, Plaintiff challenges statements that Capital One had "buil[t] out the capability of fully digital consumer banking and . . . all the fraud defenses that go along with digital banking" and that Capital One had "[a]ccelerated focus on cloud capabilities, modern software engineering and delivery, and enhanced cybersecurity capabilities." *Id.* ¶¶ 226, 229 (emphasis omitted); Ex. 1, Stmts. 6, 9. But Plaintiff has not pled that Defendants did not "accelerate" their "focus" on "enhanced cybersecurity capabilities" or that they had actually failed to build out "the fraud defenses that go along with digital banking." Once again, the occurrence

[7] Plaintiff references SEC Guidance discussing disclosure of cybersecurity risks. AC ¶¶ 212-222. As noted above, the Risk Factor Statements apprised investors in great detail as to the existence of cybersecurity risks, just as the SEC Guidance envisions. Plaintiff seems to suggest that the SEC Guidance required Capital One to discuss the Montana incidents in its 10-K. But Plaintiff fails to plead any facts suggesting the Montana incidents were "material cybersecurity incidents." In any event, the SEC's general disclosure guidance does not carry the force of law and does not impose an independent regulatory disclosure obligation. *Allen v. Administrative Review Bd.*, 514 F.3d 468, 479 (5th Cir. 2008).

of the Cyber Incident does not establish the falsity of these statements. *See Ong v. Chipotle Mexican Grill, Inc. ("Chipotle II"),* 294 F. Supp. 3d 199, 232 (S.D.N.Y. 2018) (allegations that did not "conflict with Defendants' statements regarding the . . . programs and procedures that Chipotle had in place, but merely quibble[d] with [the] execution of those programs and procedures," failed to adequately plead the statements' falsity).

Other Digital Transformation Statements do not even appear to relate directly or primarily to cybersecurity—*e.g.*, that the "digital transformation" led to "better compliance outcomes" or that "there's not a single major undertaking or challenge the business has where . . . the cloud or big data or open source software . . . can't make a huge difference in both the revenue and the expense side." AC ¶¶ 225, 228; Ex. 1, Stmts. 5, 8 (emphasis omitted). Many such statements include non-verifiable opinion/belief statements that are not alleged to be false in any event. *See, e.g.*, AC ¶¶ 223, 225–29; Ex. 1, Stmts. 4–9; *see also Nolte v. Capital One Fin. Corp*., 390 F.3d 311, 315 (4th Cir. 2004) (to plead an opinion is a false statement, the complaint "must allege that the opinion expressed was different from the opinion actually held by the speaker").

Claims based on the Digital Transformation Statements also should be dismissed on puffery grounds because they are subjective, soft, vague and non-verifiable. *See, e.g., Hillson Partners*, 42 F.3d at 210 (statements that company "was looking for record earnings" and that "sales were 'good'" constituted "soft puffing statements" not actionable under Section 10(b)).

4. The Priority Statements

The Priority Statements (Ex. 1, Stmts. 10-21) consist of statements describing the importance of cybersecurity to Capital One—often in vague, optimistic, and non-verifiable terms. Typical of the Priority Statements challenged by Plaintiff are the following:

- "We're investing in cybersecurity. This is an incredibly important area and we are putting a lot of very top talent and a lot of energy and investment into that." AC ¶ 232; Ex. 1, Stmt. 10 (quoting Mr. Fairbank);

- "… security is critical for us. The financial services industry attracts some of the worst cyber criminals so we . . . develop a security model that we believe enables us to operate more securely in the public cloud…." *Id.* ¶ 233; Ex. 1, Stmt. 11 (quoting Mr. Alexander);

- "Most important to us is the confidentiality, integrity and the availability of our data in the cloud." *Id.* ¶ 234; Ex. 1, Stmt. 12 (quoting Mr. Johnson);

- A statement on Capital One's website that "Your security is a top priority."[8] *Id.* ¶ 238; Ex. 1, Stmt. 16;

- "As a financial institution, we take the safety of our customer data incredibly seriously." *Id.* ¶ 242; Ex. 1, Stmt. 18 (quoting a YouTube video featuring non-defendant George Brady); and

- "As a financial services company entrusted with the safeguarding of sensitive information, our Board believes that a strong enterprise cyber strategy is vital to effective cyber risk management. *Id.* ¶ 243; Ex. 1, Stmt. 19 (quoting Capital One's 2018 proxy statement).[9]

(emphases omitted). Plaintiff contends that these statements "gave the misleading impression that Capital One had met and exceeded" "regulatory requirements" and "customer expectations" when in fact Capital One "sacrifice[ed] cybersecurity" by creating large data pools, granting broad access, failing to monitor data requests, and not effectively encrypting data. AC ¶ 246.

First, several of the Priority Statements are statements of opinion or belief—*e.g.*, statements explicitly framed as beliefs in Capital One's proxy statements (AC ¶¶ 243-44; Ex. 1, Stmts. 19-20) and various statements describing the importance cybersecurity to Capital One (*Id.* ¶¶ 232-34, 238, 242, 245; Ex. 1, Stmts. 10-12, 16, 18, 21). Such statements are not actionable unless Plaintiff pleads sufficient facts to establish that the speaker did not actually hold the stated belief at the time it was expressed. *See Nolte*, 390 F.3d at 315. Plaintiff has failed to do so here. Second, to the extent Plaintiff relies on the Cyber Incident to assert the falsity of these statements,

[8] Plaintiff does not cite the portion of the website from which this quote was taken, and erroneously calls it "Capital One's cybersecurity policy." *Id.* ¶ 238. The text currently appears at www.capitalone.com/applications/identity-protection/commitment/.

[9] Part of Stmt. 2—"we make your safety and security a top priority"—also falls in this category.

that approach fails because "[t]he fact that a company has suffered a security breach does not demonstrate that the company did not 'place significant emphasis on maintaining a high level of security.'" *Heartland*, 2009 WL 4798148, at *5. It is "equally plausible that [Capital One] did place a high emphasis on security but that [its] security systems were nonetheless overcome." *Id.* *See also Weil v. Dominion Resources, Inc.*, 875 F. Supp. 331, 336 (E.D. Va. 1994) (rejecting falsity of statement that "regulatory policy continues to be of fundamental importance to [defendant] because there was "no suggestion that [defendant] has regarded 'regulatory policy' unimportant").

Third, the Priority Statements clearly constitute immaterial puffery which, as noted above, is not actionable under the securities laws. *See, e.g.*, *Longman*, 197 F.3d at 685 (holding statements touting the cleanliness of defendant's grocery stores to be immaterial puffery); *In re Neustar Sec.*, 83 F. Supp. 3d 671, 676 & 680-81 (E.D. Va. 2015) (statements regarding confidence in winning bid due to "our capabilities and outstanding track record" were puffery). Such "banal and vague corporate statements" which only affirm the "importance" of cybersecurity "do not invite reasonable reliance." *See Singh*, 918 F.3d at 60.

The Priority Statements challenged by Plaintiff are textbook puffery and are not pled to be false. These statements say that Capital One makes cybersecurity "a top priority and [is] committed to protecting your personal and financial information," that Capital One was "excited" to allow "customers to share their data in a way that is secure," or that it "take[s] the safety of our customer data incredibly seriously." AC ¶¶ 210, 237, 242 (emphases omitted); Ex. 1, Stmts. 2, 15, 18. In another case in which a shareholder plaintiff tried to spin a data breach as securities fraud, the Northern District of California recently held that "generalized statements regarding the importance of privacy to users and [defendant's] general commitment to transparency and [data] protection" were "too vague and generalized to constitute the bases for misrepresentations." *In re*

Alphabet, Inc. Sec. Litig., No. 4:18-cv-06245, at 6 (N.D. Cal. Feb. 5, 2020) (copy attached as Ex. F). Courts across the country have reached similar conclusions in a variety of contexts. *See Howard v. Arconic Inc.*, 395 F. Supp. 3d 516, 547 (W.D. Pa. 2019) ("general statements about [company's] values, workplace safety, and ethics—which read like mission statements rather than guarantees—were not rendered misleading by product safety issues"); *Singh*, 918 F.3d at 63 ("general declarations about the importance of acting lawfully and with integrity" constitute "textbook" puffery); *Ocwen*, 934 F.3d at 1321-22 (same); *Chipotle II*, 294 F. Supp. 3d at 232 (statements of commitment to food safety were non-actionable).

5. Defendants' Consumer-Facing And Technical Statements Were Not Made "In Connection With" The Purchase Or Sale Of Securities.

Plaintiff's claims based on Stmts. 2, 11-13, 16, 18, 21, 24, 26 in Exhibit 1 also fail for the separate and independent reason that these statements were not made "in connection with" the purchase or sale of a security, as required under Section 10(b). *See* 15 U.S.C. § 78j(b). The Fourth Circuit has endorsed several factors articulated by other courts to determine whether the "in connection with" requirement is met. *See S.E.C. v. Pirate Inv'r LLC*, 580 F.3d 233, 244 (4th Cir. 2009). Here, the most relevant factor derives from the Second Circuit's *Texas Gulf Sulphur* decision and asks whether the challenged statements were disseminated via a medium upon which a reasonable investor would rely. *See Pirate*, 580 F.3d at 244; *see also SEC v. Tex. Gulf Sulphur Co.*, 401 F.2d 833, 862 (2d Cir. 1968) (to satisfy the "in connection with" requirement, a statement must have been made "in a manner reasonably calculated to influence the investing public.").

Capital One's Online & Mobile Privacy Statement, its "cybersecurity policy," and its Annual Privacy Notice to Credit Card Holders (AC ¶¶ 210, 238, 253; Ex. 1, Stmts. 2, 16, 26) do not meet this standard. These statements are not alleged to have been included in any communication directed at investors, such as SEC filings, but instead appear on customer-facing

pages of the Company's website. Such customer-directed communications do not satisfy the "in connection with" standard. *See In re LifeLock, Inc. Sec. Litig.*, 690 F. App'x 947, 954 (9th Cir. 2017) (statements made in advertisements "might have some probative value in an action based on consumer protection laws," but "have none in a case alleging investor fraud"); *Arconic*, 395 F. Supp. 3d at 539 (product brochures are not "a medium upon which a reasonable investor would rely" and do not meet the in connection with requirement); *cf. SEC v. Rana Research, Inc.*, 8 F.3d 1358, 1362 (9th Cir. 1993) (actionable statements are typically published in company press releases, annual and quarterly reports, analyst reports, proxy statements, and other SEC filings).

Second, Plaintiff challenges an assortment of statements made by Company officials at technology conferences or posted on YouTube. *See* AC ¶¶ 233-35, 242, 245, 251; Ex. 1, Stmts. 11-13, 18, 21, 24. Plaintiff bears the burden of alleging facts satisfying the "in connection" with requirement. *Pirate*, 580 F.3d at 244. However, he has failed to provide factual allegations necessary to make such a determination, including the subjects of these conferences, whether these conferences were public, who attended these conferences, whether investors were invited, and whether the remarks were widely disseminated. Plaintiff thus fails to allege that these statements were made in a manner reasonably calculated to reach investors. *See Intel*, 2019 WL 1427660, at *11 n.14 (the complaint failed to "allege that the product statements were directly targeted to investors or the investment community"). This pleading infirmity is compounded by the fact that many of these statements are alleged to be made by officials with IT-focused roles, and Plaintiff does not allege that they had investor-facing roles. Plaintiff has thus failed to meet its burden of satisfying the "in connection with" requirement.

B. Plaintiff's Allegations Fail To Raise A Strong Inference Of Scienter.

The Complaint also must be dismissed because it fails to meet the PSLRA's heightened standards for pleading scienter. *See* 15 U.S.C. § 78u-4(b)(2)(A). Scienter can be pled by "alleging

either intentional or severely reckless conduct." *Yates v. Mun. Mortgage & Equity, LLC*, 744 F.3d 874, 884 (4th Cir. 2014). "A plaintiff may not stack inference upon inference to satisfy the PSLRA's pleading standard" and must instead "state with particularity *facts* giving rise to a strong inference that the defendant acted with the required state of mind." *Maguire,* 876 F.3d at 548 (quoting 15 U.S.C. § 78u-4(b)(2) (emphasis in original). Crucially, a plaintiff must allege such facts as to "*each* defendant" and with respect to each alleged violation. *Teachers' Ret. Sys. of La. v. Hunter*, 477 F.3d 162, 184 (4th Cir. 2007) (internal citations omitted) (emphasis in original). "[I]f the defendant is a corporation, the plaintiff must allege facts that support a strong inference of scienter with respect to at least one authorized agent of the corporation, since corporate liability derives from the actions of its agents." *Id.*

1. Plaintiff's Allegations About Defendants' Positions And Alleged Access To Internal Information Are Insufficient.

Plaintiff's Complaint—which mentions the word "scienter" only twice—relies on generic allegations that could apply to any executive at any company. Plaintiff first alleges that:

> Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of Capital One were materially false and misleading . . . by virtue of their receipt of information reflecting the true facts of Capital One, their control over, and/or receipt and/or modification of Capital One's allegedly materially misleading statements, and/or their associations with the Company which made them privy to confidential proprietary information concerning Capital One, participated in the fraudulent scheme alleged herein.

AC ¶ 272. This style of conclusory, boilerplate pleading—which is written in the disjunctive and does not link any specific Defendant to any specific fact—is insufficient as a matter of law. *See In re Genworth Fin. Inc. Sec. Litig.*, 103 F. Supp. 3d 759, 783 (E.D. Va. 2015) ("Adding the words 'knowingly' or 'recklessly' to a factual statement is insufficient pleading.") (internal quotations omitted).

To the extent Plaintiff alleges that "Defendants" had actual knowledge of falsity "by virtue of their receipt of information reflecting the true facts of Capital One," Plaintiff fails to plead specific facts establishing Defendants' receipt of such information. As this Court held in *In re Maximus, Inc. Securities Litigation*, a plaintiff cannot plead scienter by citing "internal reports" containing information that contradicts a Company's public statements "without sufficient factual allegations to connect these reports to the Individual Defendants." No. 1:17-cv-0884 (AJT/IDD), 2018 WL 4076359, at *12 (E.D. Va. Aug. 27, 2018) (Trenga, J.) ("[T]hat contrary information existed somewhere in the company does not sufficiently show that [defendant] had scienter with respect to [the alleged misrepresentation]."). *See also Teamsters Local 445 Freight Div. Pension Fund v. Dynex Capital Inc.*, 531 F.3d 190, 196 (2d Cir. 2008) ("[W]here plaintiffs contend defendants had access to contrary facts, they must specifically identify the reports or statements containing this information.") (internal citation and quotation marks omitted). The plaintiff in *Maximus* provided more detail regarding the alleged reports than does the Complaint in this case. For example, the *Maximus* plaintiff at least identified the reports by name ("Operation Reports"), provided some level of detail regarding their contents, and alleged that there were inconsistencies between the reports and the defendants' public statements. *See* 2018 WL 4076259, at *2, *12. Here, by contrast, Plaintiff does not even bother to specify what information Defendants allegedly received, other than that it "reflect[ed] the true facts of Capital One"—whatever that means.[10]

Plaintiff also asserts, in conclusory fashion, that (i) Defendants' "associations with the Company . . . made them privy to confidential proprietary information concerning Capital One" and that (ii) the "Individual Defendants, who are the senior officers and/or directors of the Company, had actual knowledge of the . . . falsity of the material statements . . . and intended to

[10] Plaintiff also fails to specify *which* Individual Defendants allegedly received such information.

deceive Plaintiff and the other members of the Class." AC ¶¶ 272-73. These allegations are also plainly inadequate. "Guesswork of this kind, based on the position of the Defendants is insufficient under the Reform Act." *Smith v. Circuit City Stores, Inc.*, 286 F. Supp. 2d 707, 715 (E.D. Va. 2003) (citing *First Union*, 128 F. Supp. 2d at 888); *see also Schwab v. E*Trade Fin. Corp*., 285 F. Supp. 3d 745, 757 (S.D.N.Y. 2018), *aff'd*, 752 F. App'x 56 (2d Cir. 2018). For this reason, "[c]ourts have routinely held that corporate executives' access to information and internal affairs is not enough to demonstrate scienter under the PSLRA." *Lerner v. Northwest Biotherapeutics*, 273 F. Supp. 3d 573, 593 (D. Md. 2017) ("[A] defendant's position of control in a company, without more, is insufficient to establish scienter.").

2. The "Former Employee" ("FE") Allegations Fail To Support A Strong Inference Of Scienter.

The Prior Alleged Incidents. The only FE allegation that even arguably bears on the general concept of scienter is FE 3's allegation regarding prior "cybersecurity attacks and data breaches," but this is insufficiently particularized to give rise to an inference of scienter. Plaintiff does not even specify whether these were unsuccessful, attempted "attacks" or actual "breaches" and instead treats the two as if they were the same. Plaintiff alleges that during FE 3's tenure, Capital One suffered upwards of "20 cyber attacks per month" and that "FE 3 reported to Johnson data from his team about attacks on Capital One's server." AC ¶¶ 149-50. In the very next sentence, however, Plaintiff states "FE 3 understands that in turn, *these breaches* were reported to Defendant Alexander." *Id.* ¶ 150 (emphasis added). Without pleading specific facts, equating "attacks on Capital One's server" with "breaches" is a mistake. There is an obvious distinction between an attack that is rebuffed by a company's defenses and a breach.[11] And even successful

[11] Capital One's public risk factor disclosures warned investors that "[l]ike other financial services firms, Capital One['s networks] . . . continue to be the subject of attempted unauthorized access

attacks may be of a completely different type, severity, or risk profile as future breaches to render them meaningless for any analysis of scienter. But even setting these critical distinctions aside, a confidential witness's allegation that unnamed "attacks" were reported to Mr. Johnson does not raise a strong inference of scienter where Plaintiff fails to provide any detail regarding when these reports were allegedly made or the time, place, scope, or success of such attacks. *See Pipefitters Local No. 636 Defined Ben. Plan v. Tekelec*, No. 5:11-CV-4-D, 2013 WL 1192004, at *12 (E.D.N.C. March 22, 2013) (rejecting inference of scienter based on allegation that defendant received "scorecards" relating to revenues and the timing of payments because plaintiffs failed to "allege anything further regarding the details on the . . . scorecards," including any information that would contradict defendants' public statements).

The allegation that "FE 3 understands . . . these breaches were reported to Defendant Alexander" must also be rejected because it lacks sufficient indicia of reliability. AC ¶ 150. It is well established that a court may not consider allegations based on a confidential witness in the absence of facts that "support the probability that a person in the position occupied by the source would possess the information alleged." *Hunter*, 477 F.3d at 174 (internal citation omitted); *see also Inst'l Invs. Grp. v. Avaya, Inc.*, 564 F.3d 242, 263 (3d Cir. 2009) (recommending that courts "steeply" discount confidential witness allegations that lack corroboration, a strong "basis of knowledge," a high level of detail, and other supportive indicia). Here, "none of the [FEs] had contact with [Alexander]" and thus "cannot testify as to what [Alexander] knew." *City of Pontiac Gen. Employees' Ret. Sys. v. Stryker Corp.*, 865 F. Supp. 2d 811, 834 n.9 (W.D. Mich. 2012). *See also Tekelec*, 2013 WL 1192004, at *12 ("Absent CW6's personal knowledge, the court declines

. . . , hacking, malware, ransomware, phishing . . . , and other forms of cyber-attacks." *See, e.g.*, Ex. A at 24, cited generally, AC ¶ 218.

to credit this inference in support of scienter."). Neither FE 3 nor any of the other FEs is alleged to have reported directly or indirectly to Mr. Alexander. *See* AC ¶¶ 31-33. Nor does the Complaint plead facts to substantiate FE 3's *personal* knowledge of what was reported to Mr. Alexander.

More fundamentally, Plaintiff does not provide enough detail to explain how knowledge of these purported "attacks" or "breaches" would contradict any of Capital One's public statements. *See In re DRDGOLD Ltd. Sec. Litig.*, 472 F. Supp. 2d 562, 572 (S.D.N.Y. 2007) (finding confidential witness allegation that there were "many undisclosed illegalities" insufficient because plaintiffs did "not give any further specifics regarding the sum and substance of these 'illegalities.'"). For instance, Plaintiff does not even attempt to compare these prior "attacks" or "breaches" to the Cyber Incident or to any of the purported vulnerabilities that Plaintiff contends made "a hack like the Data Breach inevitable." AC ¶ 17. Without particularized allegations that Defendants "had access to information that would suggest that their public statements were not accurate," *In re Under Armour Sec. Litig*., 342 F. Supp. 3d 658, 691 (D. Md. 2018), Plaintiff's contention that Capital One suffered "near-constant cybersecurity attacks," AC ¶ 149, only confirms that banks like Capital One were targeted by hackers. But this was no secret—indeed, Plaintiff alleges that Mr. Alexander openly acknowledged that the "financial services industry attracts some of the worst cyber criminals." *Id.* ¶ 233; Ex. 1. Stmt. 11; *see also* Ex. A at 24.

The Remaining FE Allegations. The remaining FE allegations do not bear on the Individual Defendants' scienter at all and are instead criticisms of the way in which Capital One was managed. For instance, FE 2 describes Capital One's cybersecurity as "lackadaisical" and criticizes the Company for, alternately, "not hav[ing] a map of its internal network" or for not "incorporat[ing newly acquired] data lakes into its network map." AC ¶¶ 129-30, 138. FE 1 similarly finds fault with Capital One for "delegat[ing] authority for security to individual lines of

business" and allowing them to "creat[e] their own security protocols and access controls." *Id.* ¶¶ 127, 132. Such allegations "amount to no more than former employees who . . . disagreed with management's decisions" and thus fail to raise a strong inference of scienter. *Druskin v. Answerthink, Inc.*, 299 F. Supp. 2d 1307, 1334 (S.D. Fla. 2004). Even if the business practices challenged by these former employees constituted negligence—and they do not—the "inference that [Defendants] were negligent in discharging their duties . . . is not enough to survive a motion to dismiss" in a securities case. *Yates*, 744 F.3d at 894. These criticisms also fail to plead scienter because none of them is alleged to have been reported to any Individual Defendant. *See Phillips*, 2015 WL 1457980, at *6 (rejecting CW allegations where "Plaintiff does not allege . . .what information the [CW] reported to [Defendant].").[12]

3. Plaintiff's Other Allegations Fail To Raise The Required Strong Inference.

The Complaint is also notable for what it does *not* allege. First, Plaintiff does not and cannot allege that any insider trading took place. This omission is significant because "[a]llegations of personal financial gain 'may weigh heavily in favor of a scienter inference.'" *Yates*, 744 F.3d at 890 (citing *Tellabs*, 551 U.S. at 325). Second, Plaintiff makes virtually no allegations as to the Defendants individually and instead groups them together, without accounting for differences in their respective roles and responsibilities. *See, e.g.*, AC ¶¶ 272-73 (alleging that "Defendants acted with scienter" and that "Individual Defendants . . . had actual knowledge of the

[12] Plaintiff's allegations about an "illegal[] purchase … on the Dark Web" of data stolen from Yahoo! (AC ¶¶ 139-45) do not support any inference of scienter. First, these allegations have no bearing on *any* of the challenged statements regarding Capital One's cybersecurity practices, and for that reason alone fail to raise an inference of scienter. *See Phillips*, 2015 WL 1457980, at *4 (disregarding CW allegations "because the facts that this confidential source alleges are . . . immaterial"). Second, Plaintiff pleads no facts indicating that the alleged data purchase or other dealings with the "Russia-Affiliated Vendor" were reported to any Individual Defendant—or indeed, to anyone other than FE 2's unnamed "superior." *See* AC ¶¶ 32, 142. Plaintiff has failed to "provide direct allegations concerning Defendants' knowledge," as required by the PSLRA. *Kiken v. Lumber Liquidators Holdings, Inc.*, 155 F. Supp. 3d 593, 606 (E.D. Va. 2015).

material omissions and . . . [mis]statements"). A long line of cases establishes that such generalized, group pleading does not satisfy the PSLRA's particularity requirement. As the Fourth Circuit has held, the "aggregation of defendants without specifically alleging which defendant was responsible for which act" is "impermissible" and "indicative of the insufficiently particular character of the complaint." *Juntti v. Prudential-Bache Sec., Inc.*, 993 F.2d 228 (4th Cir. 1993); *accord Tekelec*, 2013 WL 1192004, at *6.[13]

Finally, in assessing scienter allegations, the Court must make a comparative inquiry to determine whether "the malicious inference is at least as compelling as any opposing innocent inference." *Yates*, 744 F.3d at 885. Here, Plaintiff has not pled facts suggesting that the fraudulent inference Plaintiff seeks to draw is as compelling as the opposing inference that Capital One genuinely believed cybersecurity was important and emphasized it accordingly, but nonetheless fell victim to a cyber-attack. That Capital One's SEC filings warned of precisely this risk further undercuts any inference that Defendants intended to deceive investors.[14]

V. CONCLUSION

For the foregoing reasons, the Defendants respectfully request that the Court dismiss the Complaint with prejudice.

---

[13] To plead scienter as to Capital One, Plaintiff must allege facts that raise a strong inference of scienter as to an "authorized agent" who "made" a misleading statement. *In re Computer Sciences Corp. Sec. Litig.*, 890 F. Supp. 2d 650, 664–65 (E.D. Va. 2012); *accord Matrix Capital Management Fund, LP v. BearingPoint, Inc.*, 576 F.3d 172, 189 (4th Cir. 2009) (plaintiff must plead facts raising a strong inference that "at least one corporate agent . . . acted with the required state of mind"). Plaintiff's allegations concerning the Individual Defendants are insufficient for reasons discussed above. And Plaintiff's conclusory allegations that scienter of non-defendants Brady, Hieronimous, Crawford, Norris, and Blackley is "imputed to the Company under respondeat superior," AC ¶ 275, are likewise insufficient because Plaintiff fails to plead particular facts sufficient to raise a strong inference that any of these non-defendants acted with scienter.

[14] Because the Complaint fails to state a claim for violation of Section 10(b) or Rule 10b-5, the Section 20(a) claim likewise fails. *See Hunter*, 477 F.3d at 188.

Respectfully submitted this 18th day of February 2020.

/s/
David L. Balser (*pro hac vice*)
Michael R. Smith (*pro hac vice*)
Benjamin Lee (*pro hac vice*)
Kevin J. O'Brien (VSB No. 78886)
Peter Starr (*pro hac vice*)
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
mrsmith@kslaw.com
blee@kslaw.com
kobrien@kslaw.com
pstarr@kslaw.com

Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
TROUTMAN SANDERS LLP
1001 Haxall Point
Richmond, VA 23219
Tel.: (804) 697-1200
Fax: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
TROUTMAN SANDERS LLP
401 9th Street, NW, Suite 1000
Washington, DC 20004
Tel.: (703) 734-4334
Fax: (703) 734-4340
mary.zinsner@troutman.com

Counsel for Defendants Capital One Financial Corporation, Richard Fairbank, and Robert Alexander

/s/
Gregory S. Bruch (*pro hac vice* application forthcoming)
Lara N. Burke (VSB No. 85601, appearance forthcoming)
BRUCH HANNA LLP
1099 New York Ave., NW
Suite 500
Washington, DC 20001
Tel.: (202) 969-1631
Fax: (202) 969-1625
gbruch@bruch-hanna.com
lburke@bruch-hanna.com

Counsel for Defendant Michael Johnson

CERTIFICATE OF SERVICE

I hereby certify that on February 18, 2020, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/
David L. Balser (*pro hac vice*)
KING & SPALDING LLP

Counsel for Defendants Capital One Financial Corporation, Richard Fairbank, and Robert Alexander